*BY ORDER OF THE COMMANDER*
*AIR FORCE MATERIEL COMMAND*


*AIR FORCE INSTRUCTION 31-210*

*AIR FORCE MATERIEL COMMAND*
*Supplement 1*

*21 January 2000*

*Security*

# *AIR FORCE ANTITERRORISM/FORCE PROTECTION (AT/FP)PROGRAM STANDARDS*

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the HQ AFMC WWW site at: http://afmc.wpafb.af.mil. If you lack access, contact the Air Force Publishing Distribution Center (AFPDC).

---

OPR: HQ AFMC/SFOC (Mr. Tommy L. Webb)

Certified by: HQ AFMC/SF
(Col Hubert G. Mitchell)

Supersedes AFI 31-210/AFMCS 1, 11 May 98

Pages: 15
Distribution: F

---

This supplement implements AFI 31-210, *The Air Force Antiterrorism/Force Protection (AT/FP) Program Standards, 1 August 1999.* It expands on the guidance in the Air Force instruction, delineates specific responsibilities, and applies to all organizations within AFMC to include government-owned, contractor-operated (GOCO) facilities. It does not apply to US Air Force Reserve or National Guard units. The terms "must," "shall," and "will" denote mandatory actions in this supplement. Send comments and suggested improvements on AF Form 847, Recommendation for Change of Publication, through unit force protection channels to HQ AFMC/SFO, Building 266, Room N208, 4225 Logistics Avenue, Wright Patterson AFB OH 45433-5760.

## *SUMMARY OF REVISIONS*

This document is substantially revised and must be completely reviewed.

**AFI 31-210, 1 August 1999, is supplemented as follows:**

1.6. AFMC Installation/Site commanders are responsible for the AT/FP program at their respective installation or site.

1.8. (Added) Operations Security (OPSEC). The goal of OPSEC is to control information and observable actions about friendly force capabilities, limitations, and intentions so as to prevent or control their exploitation by an adversary. OPSEC must be incorporated throughout the entire AT/FP program. Air Force OPSEC policy can be found in AFI 10-1101 and the AFMC Supplement thereto.

3.1.1.1. HQ AFMC/SF is the OPR and action agency for AFMC AT/FP matters and policy. In addition, SF chairs the Force Protection Working Group (FPWG) and provides a team leader and two force protection specialists to the Headquarters Vulnerability Assessment Team (AFMC VAT).

3.1.1.2. (Added) AFMC/CC will establish a HQ AFMC Force Protection Senior Steering Group (FPSSG) chaired by AFMC/CV. The FPSSG is the AFMC body responsible for ensuring integration of security disciplines, Infrastructure Assurance, and Information Assurance to produce an effective FP program. The FPSSG combines all Force Protection stakeholders into one comprehensive decision-making body to better support AFMC's Force Protection efforts. The Installations and Support Chief Operating Officer (AFMC/CE) is the lead organization for FPSSG meetings and action items. The FPSSG is comprised of selected leaders, in the grade of 0-6 or above, who have decision authority, representing CE, DO, IG, IN, JA, AFOSI, SC, SF, SG, FM, LG, DP, IA, and XP.

3.1.1.3. (Added) HQ AFMC/SF will establish a FPWG consisting of representatives from CE, DO, IG, IN, JA, AFOSI, SC, SF, SG, and XP. Additional headquarters and/or functional representatives may participate in FPWG proceedings as required. The FPWG is charged with the overall effectiveness of the command's force protection program to include tracking terrorist capabilities and disseminating threat information. SF will serve as Chairperson of the FPWG. Within the FPWG, AFOSI, IN and SF make up the Threat Working Group and are responsible for assessing threat information.

3.1.3. HQ AFMC/SG will provide a fully qualified operation readiness specialist to support the Headquarters AFMC VAT. Provide core members to the Headquarters FPSSG and FPWG with medical and WMD expertise as required.

3.1.5. HQ AFMC/DO provides a core member to the Headquarters FPWG with operational expertise as required.

3.1.5.1. HQ AFMC/IN provides core members to the Headquarters FPSSG and FPWG with international terrorism expertise as required.

3.1.6. AFMC Public Affairs Offices will encourage the use of all available internal information resources to support DoD-directed briefings and training. Such resources include, but are not limited to, installation bulletin boards, official publications, commercial enterprise newspapers, internal computer Local Area Networks (LAN) and installation television assets such as the Commander's Access Channel. Prepare a generic news release applicable to terrorist incidents in concert with the installation commander. Establish and maintain liaison with local media.

3.1.7. HQ AFMC/JA provides core members to the Headquarters FPSSG and FPWG to provide legal expertise as required.

3.1.8. AFOSI (1 FIR) will provide a fully qualified terrorist options specialist to support the Headquarters AFMC VAT. Provide core members to the Headquarters FPSSG and FPWG to provide counterintelligence expertise as required.

3.1.9. HQ AFMC/LG provides a core member to the Headquarters FPSSG to provide logistical expertise as required.

3.1.10. HQ AFMC/CE provides fully qualified structural and infrastructure engineers to support the Headquarters AFMC VAT. Be the lead organization for the Headquarters FPSSG and provide core members to the Headquarters FPSSG and FPWG with civil engineering and WMD expertise as required.

3.1.12. (Added) HQ AFMC/XP provides core members to the Headquarters FPSSG and FPWG with plans expertise as required.

3.1.13. (Added) HQ AFMC/DP provides a core member to the Headquarters FPSSG with personnel expertise as required.

3.1.14. (Added) HQ AFMC/FM provides a core member to the Headquarters FPSSG with financial expertise as required.

3.1.15. (Added) HQ AFMC/IG provides core members to the Headquarters FPSSG and FPWG with force protection inspection expertise as required.

3.1.16. (Added) HQ AFMC/SC provides core members to the Headquarters FPSSG and FPWG with information assurance expertise as required.

3.1.17. (Added) HQ AFMC/SE provides a core member to the Headquarters FPSSG with safety expertise as required.

3.2.3. Installation/Site Commanders will provide HQ AFMC/SF a copy of their supplement within 120 days from the date of this supplement.

3.2.4. Installation/Site Commanders must budget for force protection requirements during the Program Objective Memorandum (POM) process.

3.3.1. Commanders and directorate heads are responsible for the implementation of DoD AT/FP policies within their organization. The term "Commanders" refers to those individuals in the chain of command from AFMC/CC down to the installation/site/unit level for permanent and temporary operations or locations. Each unit commander, tenant unit agency chief or commander, or equivalent staff agency chief responsible for protection level resources must ensure their AT/FP program meets Air Force and DoD protection criteria.

3.3.1.1. (Added) HQ AFMC/JA determined GOCOs (Air Force Plants) are not installations. However, as a matter of policy, GOCOs must implement an AT/FP program to combat the local terrorist threat and support the US Air Force AT/FP program. ASC/CC will ensure a day-to-day, contingency and wartime AT/FP program is established for all GOCOs tailored to the local mission, GOCO organizational infrastructure, conditions, the terrorist threat, and the national security environment. Since this is a new requirement, ASC/CC shall present the tailored GOCO AT/FP program to the FPSSG within 180 days from date of publication of this supplement.

3.3.4.1. Installation-wide antiterrorism exercises (both operational and command post) will be conducted semiannually, as a minimum. Conducting and evaluating these exercises together may fulfill this requirement. The exercises will be used to test and evaluate the installation's ability to respond to the local terrorist threat. Exercises will test a broad range of required THREATCON actions specified within the installation's local plans and may be combined with other base exercises such as a MARE, BROKEN ARROW, etc.

3.3.4.2. Incidents of terrorism and crime will generate external media interest. In response to queries concerning a possible or real terrorist threat at a particular activity, installation, or community, the commander may acknowledge that increased security measures have been or will be taken without going into specific details regarding the measures being taken. In other words, it may be appropriate and operationally sound to acknowledge the obvious. For example, increased security measures such as additional guards at the gate and/or more stringent identification checks are usually obvious to the public, and acknowledgement may serve to send a positive message of increased readiness. Commanders must exercise care and prudent judgement in any discussion of these or other security measures to preclude revealing tactics and techniques that an adversary could exploit. Practice good operations security (OPSEC).

3.4.5. Installation/Site Commanders will ensure all agreements for local emergency support; e.g., fire, police, medical, etc., are formally coordinated for their installations/sites. Review of agreements is a part of the FP vulnerability assessment process.

3.5.2. Commanders may use existing plans to implement AT/FP programs. Plans shall address areas outlined in DoD Standard 2 as supplemented, and include these additional areas to meet security requirements (note: this list is not all inclusive): detail media control during terrorist incidents, detail THREATCON procedures and identify a means to rapidly advise all units of THREATCON changes, and must incorporate all DoD elements and personnel for whom the installation/activity has force protection responsibility. Commanders are encouraged to consider use of the installation-planing template in developing/revising their installation plans. This template is available to download thru http://nmcc20a.smil.mil/~dj3cleap/j34.html.

3.6.3. HQ AFMC/SF schedules JSIVA, AF and AFMC vulnerability assessments of AFMC installations and sites through HQ AF/XOFP. The schedule will be coordinated with the HQ AFMC/IG Gatekeeper and the respective installation /site commander.

3.6.3.1. (Added) Installation/Site Commanders must fix AT/FP vulnerabilities identified during DoD Standards 6 and 14 vulnerability assessments; especially those that are procedural or low cost and would improve the AT/FP posture. Conversely, high cost improvements must be reviewed in context with threat and risk assessment; planned for, and programmed.

3.6.5. HQ AFMC will conduct independent vulnerability assessments of AFMC installation/sites in addition to those conducted by the AF team and the JSIVA. VAs must ensure all tenant organizations (on the installation/site or remote but administratively attached) are integrated into the force protection plan and afforded the same level of FP support as AFMC units. AFMC vulnerability assessments are not required to physically assess every single activity on the installation, but instead must assess an appropriate number that will indicate a prudent level of FP is in place for the entire installation/site.

3.6.5.1. (Added) AFMC VAT composition may vary based on the type of site or installation being assessed. The assessment team shall consist of a team chief (SF lead), force protection specialist (two), structural engineer, infrastructure engineer, operational readiness specialist and a terrorist options specialist. Other functional experts may augment the team as needed. Augmentation will depend on type of assessment required, the nature of the installation's/site's mission, the terrorist threat level, and the THREATCON. Assessments may require expertise in preventive medicine, linguistics, chemical/biological/radiological weapons effects, emerging AT/FP technology, explosive ordnance disposal, Information Operations (IO), special warfare, or other specialties as determined by the commander or directed by HQ AFMC/SF. Regardless of team composition, the team must have expertise in these areas: (1) Physical Security, (2) Structural Engineering (Weapons Effect Specialist), (3) Operational Readiness, (4) Law Enforcement and Security Force Operations, (5) Infrastructure Engineering, and (6) Counterintelligence/ Intelligence.

3.7.4. Commanders shall use intelligence (to include terrorist, criminal and other potential threats, as well as the security environment of the local area) as a tool in developing/updating plans and programs to protect assets within their installation or site.

3.8.2.2. Installation/Site Commanders shall task the appropriate intelligence/counterintelligence organizations under their command to collect, analyze, and disseminate terrorist threat information as appropriate. Commanders at all levels shall ensure personnel under their command properly report information on events, or situations that could pose a threat to the security of DoD personnel and resources.

3.9.3. Installation/Site Commanders shall ensure terrorist threat assessments for their area of responsibility are incorporated in the risk assessment development process and included in appropriate plans.

3.10.3. The Installation/Site commander will develop a formal charter outlining the purpose, roles and responsibilities of the force protection working group (FPWG).

3.11.1. (Added) The THREATCON development process will incorporate the procedures outlined in paragraph 3.12.2 as supplemented.

3.12.2. Installation/Site Commanders decide when to go to higher THREATCONs based on local conditions. Downward directed THREATCON changes for AFMC units will come from or through AFMC/CC. Tenants on AFMC bases should coordinate owning MAJCOM/Service THREATCON changes and seek concurrence from the host prior to implementing the THREATCON. Installation Commanders will consider the request, determine local threats, and make a base-wide determination. In those instances where local threats are absent, commanders will seek clarification from AFMC prior to increasing THREATCONs. There should only be one THREATCON on AFMC bases with final determination by the installation/site commander.

3.12.3. After action reports, containing comprehensive discussion of lessons learned will be forwarded to HQ AFMC/SF within 30 days of a reported terrorist threat or terrorist incident.

3.13.1.2. Installation plans will include the verbatim DoD measures listed in Attachment 3 augmented with local measures.

3.13.1.3. Commanders at all levels shall establish local measures to transition between THREATCONs.

3.13.1.4. Installations will develop and implement local Random Antiterrorism Measures (RAMs). To be effective, RAMs need to be utilized in THREATCONs Normal to Bravo. As a minimum, utilize the RAMs contained within AFI 31-210, Attachment 3. Fifty-one security measures are listed for THREATCON Alpha through Delta with one measure in each THREATCON, with the exception of Bravo which has two, to be determined. Locally devised measures above and beyond THREATCON Charlie may be used. RAM execution will be broad based and involve a variety of career fields and personnel. Locally developed measures will follow the format provided in AFI 31-210, Attachment 3. In other words, list the DoD measure and supplement with additional local measures. For example: AFI 31-210, Attachment 3, paragraph A3.2.2.1 depicts DoD Measure 1. Paragraphs A3.2.2.1.1 and A3.2.2.1.2 are Air Force added supplemental measures.

3.14.2. The Security Force Commander is the OPR for conducting physical security vulnerability assessments within AFMC. Include off-site activities (outside-the-fence) as part of the assessment. Conduct assessments every two years or when significant changes occur. Units with nuclear missions will update their physical security vulnerability assessment every twelve months. Initial Standard 14 assessments will be completed by December 2000 with the respective two and one year cycle starting thereafter. As a minimum, assessment team composition shall include Security Forces (lead), AFOSI, Civil Engineering, Intelligence, Medical and Communications. A qualified representative from the Wing Information Protection Office will conduct the communications portion of the physical security vulnerability assessment. Results of the Information Protection Assessment Program review conducted IAW AFI 33-230 will supplement the physical security vulnerability assessment. Use the JSIVA checklist, the checklist provided as an attachment to DoD 0-2000.12-H, Feb 93 and AFOSI Pamphlet 71-123, to accomplish the assessments. Classify assessment vulnerability reports pursuant to the JSIVA Security Classification Guide, 1 Sept 97. Forward a courtesy copy of the completed DoD Standard 14 assessment to HQ AFMC/SF within 90 days after the assessment.

3.15.3. Plans must include tenant activities and/or DoD elements and personnel for whom the commander has force protection responsibility. Where there are multiple command authorities on the installation, the designated installation/site commander is responsible for coordinating the physical security plans for all units on the installation. Review these program plans on a semi-annual basis or when the local threat level changes.

3.16.1. Local command authorities will exercise all portions of their AT/FP plans semi-annually. Exercises shall involve local off-base agencies to the greatest extent possible, and encompass duty and non-duty hours. Exercises shall include all tenant activities and/or DoD elements and personnel for whom the commander has force protection responsibility.

3.17.2. Commanders shall routinely (or when the Terrorist Threat Level changes) review the effectiveness of day-to-day physical security measures under the existing THREATCON posture. As a minimum, consider access control, patterns of population concentrations for both work and social purposes, and sensitive areas that may be lucrative targets for terrorists and criminals.

3.18.2. Commanders shall ensure all DoD personnel assigned who live in off-installation housing receive the following guidance for selecting private residences to mitigate risk of terrorist attack. A Housing Office, if available, should be the installation/site commander's executive agent to ensure guidance is provided.

**Off-Installation Housing Checklist**

**Off-Installation Housing Considerations:**

1. Give preference to residences that maximize safety and security while minimizing the need for security upgrades.
2. For single family residences, preferences should be given to those with a perimeter barrier, such as a wall or fence that deters access to the property.
3. Preference should be given to residences with off street parking, and ideally secured in some manner.
4. Entrance areas and apartment hallways should be illuminated.
5. Entrances should have a substantial door.
6. Each entrance should have a capability to permit the occupant to identify visitors without opening the door.
7. Each entrance should have a deadbolt lock. A double cylinder lock should be used if placed within 40 inches of a glass side light or door window; fire safety rules should be considered when installing this type of lock.
8. Accessible window/opening should have a latching or locking mechanism.

**Critical and High Threat Level Areas will also include the following (optional at lower threatlevels):**

1. Residences having multiple access routes to arterial roads should be given preference.
2. Grounds adjacent to the building faÁade and all entrance areas and apartment hallways should be illuminated.

3. Grills deemed adequate for local conditions are required on all accessible ground floor windows/ openings where patterns of violence commonly used forced entry. Existing window barriers such as roll-down or hinged shutters or alarmed openings can preclude the need for grills.
4. Grilled residences above the fourth floor require a secondary means of escape.
5. Residences should be alarmed to protect accessible window/openings and doors.
6. A safe haven should be considered where the threat includes forced entry into residences accompanied by physical harm to an occupant residences above the first floor are excluded.

3.19.3. Results of this evaluation must be documented and maintained on file for review by higher headquarters assessment officials pursuant to DoD Standard 6.

3.19.3.1. (Added) AFMC assigned forces located within or transiting geographical CINC AORs will comply with that CINC's established requirements and guidance governing off-installation billeting.

3.20.2. Refer to the Interim Department of Defense Antiterrorism/Force Protection Construction Standard.

3.20.2.1. (Added) The installation/site SF may convene the FPWG to seek additional expertise from this forum in the review and coordination of new construction projects and existing building rehabilitation plans.

3.21.2. These inputs shall be used to determine if facilities/sites, either currently occupied or under consideration for occupancy by DoD personnel, can adequately protect occupants against terrorist attacks.

3.22.2. Persons conducting environmental assessments will be fully qualified bioenvironment engineers (43E3) and/or Public Health Officers (43H3).

3.23.4. Installation placement of the AT/FP Officer and alternate at AFMC field activities is at the commander's discretion; however, commanders should consider collocating the AT/FP Officer and alternate with force protection or program protection personnel to ensure effective implementation across organizational and functional lines. In accordance with the HQ AF/XOF approved unit structure the Installation Security Section (ISS) combines what was formerly the physical security, resource protection, and antiterrorism staff functions into a single section under the force protection operations branch. The person appointed may be an officer, NCO, DoD civilian, or for those installation/sites with contracted security, a DoD contractor. Grade criteria for the AT/FP Officer and alternate should generally target military 0-2/3, E-6, or DoD civilian GS-9. The installation/site commander based on mission need may waive target grades. Once the AT/FP Officer and alternate have been designated, forward a courtesy copy of the appointment letter containing the person's name, SSN, security clearance, duty phone number and e-mail address to HQ AFMC/SF. Update appointment letters as changes occur.

3.23.4.1. (Added) Commanders are strongly encouraged to qualify individuals in writing who have experience, education, training, etc. to serve as their AT/FP Officer and alternate, and exempt them from Level II training. Those appointed installation AT/FP Officers unable to be qualified by the commander should attend Level II training within 90 days of appointment.

3.23.5. Installation Commanders must budget for training to meet their Level II training requirement to ensure proper coverage of overseas deployments. AFMC/SF will only fund Level II training for the **installation** AT/FP Officer and alternate.

3.24.8.1. Commanders shall develop written procedures to ensure proof of Level I training is part of the TDY order/leave authenticating process. Personnel, to include family members, who have not completed

Level I AT/FP training with special emphasis on AOR-specific threat and medical threats will not be issued orders for overseas travel (deployed, PCS, TDY or leave). The Joint Staff Guide 5260 is available via GCCS on the J-34 Combating Terrorism web site http://nmcc20a.nmcc.smil.mil/dj3cleap/j34pubsdocs/j34/pubsdoc.html. Local reproduction is authorized.

3.24.8.1.1. (Added) AFMC organizations **must** consider AT/FP training for contractors where these personnel are permanently assigned or perform temporary duty overseas. Contracting documents shall direct the contractor to conduct and document Level I Antiterrorism Awareness Training for these personnel prior to departure for overseas travel. DoDD 2000.12, Antiterrorism/Force Protection (AT/FP) Program, and the Defense Federal Acquisition Regulation Supplement, DFARS 252.225-7042/7043, reflects current DoD AT/FP guidance for defense contractors.

3.24.8.4. Commanders and directorate heads must ensure their personnel receive annual force protection training. Annual force protection training is accomplished in the workplace by unit trainers. The HQ AFMC AT/FP Awareness briefing and the video "You May Be the Target" are tools used to conduct the annual awareness training. Use this IP address http://dodimagery.afis.osd.mil to order the video “You May Be the Target.” Document AT/FP awareness training in the same manner as other ancillary training. Training documentation is subject for review during vulnerability assessments conducted pursuant to DoD Standards 6 and 14.

3.24.9. Units needing Level II training will schedule the requirement with HQ AFMC/SFXR. Personnel selected to attend the Level II course must be prioritized as follows: (1) installation AT/FP Officer and alternate, (2) key leadership assigned to UTCs, and (3) other specialties on the installation key to successful UTC deployment, i.e., combat logistics, communications, prime beef, medical personnel and other unique teams. Submit prioritized Level II training requests to HQ AFMC/SFXR under wing commander or equivalent signature. Requests must include full name, rank/grade, SSN, security clearance, and duty phone to facilitate orders preparation.

3.24.12. All AFMC military, civilian, and contractor personnel are responsible for understanding the AT/FP concept and the terrorist threat to AFMC personnel and facilities. Each person must apply this understanding daily when carrying out of his or her assigned duties. Unit antiterrorism awareness training programs must be designed to foster a continuing appreciation of the importance of AT/FP in this command.

3.25.3. Procedures will prohibit the issuance of orders for overseas travel (deployed, PCS, TDY or leave) for those personnel who have not received Level I AT/FP training with special emphasis on AOR-specific threat and medical threats.

3.26.2. The FPSSG, based on threat information provided by AFOSI (1 FIR), will recommend to AFMC/CC for approval those positions that should be considered high-risk billets.

3.26.4. Executive officers, executive secretaries, and others responsible for accomplishing itineraries for general officers and DAF civilian equivalents are responsible for marking travel itineraries for official use only (FOUO) or classifying the itineraries confidential when required. The itinerary classified by line shall read:

**Derived From: AFI 31-210, 1 Aug 99**

**Declassify On: On completion of Trip**

3.28.3. As a part of the response plan, commanders are encouraged to develop a set of recognizable alarms for potential emergencies. Each alarm should have its own set of reactions, a means to immedi-

ately sound the alarm, and commanders should conduct frequent drills to familiarize all personnel with individual responsibilities during a potential emergency.

3.29.2. Installation/Site Commanders may need to include special security arrangements to protect DoD personnel and their family members living off base. Close coordination with other U.S. Government agencies and local authorities is essential to ensure effective allocation of security resources and protection of DoD personnel.

3.30.3. Installation/Site Commanders shall consult with their servicing AFOSI detachment if executive protection and protective services are needed.

3.31.1. Installation/site commanders shall task the appropriate intelligence/counterintelligence organization under their command to collect, analyze, and disseminate terrorist threat information pertaining to the potential terrorist use of WMD. Commanders at all levels shall ensure personnel under their command properly report information on events, or situations that could pose a threat to the security of DoD personnel and resources.

3.32.1. As a minimum, assessments should include information from intelligence, logistics, medical, physical security, facility engineering, meteorological, explosive ordnance disposal, and NBC staff elements. The entire range of potential terrorist weapons of mass destruction (WMD) use should be considered when conducting assessments. Threats from commercial chemical, biological, nuclear, and radiological sources should be included as well as traditional military agents. Examples of vulnerabilities include: (1) Individual protective clothing and equipment, (2) Collective protection equipment and facilities, (3) Medical response and emergency services capability, (4) Training of personnel, (5) Physical security and protective barriers, (6) Facility design and construction, (7) Early warning and detection, (8) Alarms and attack warning, (9) Threat intelligence, (10) Preventive medicine and vaccination programs, (11) Sustainment operations and follow on support, (12) Storage of bulk hazardous material, (13) Explosive ordnance disposal response capability/availability and (14) Food and water sources.

3.33.2.1. Report will be sent to HQ AFMC/SFO who will in turn pass the information to AFSFC/SFP.

3.33.2.7. (Added) As a part of the overall installation/site AT/FP plan, commanders should address the WMD threat and exercise the WMD part of the plan to determine its effectiveness in mitigating the effects of an attack. In addition to providing crisis action and consequence management procedures, planning should include pre-attack measures and consideration for collateral damage a WMD may have on adjacent facilities and surrounding communities. Plans should provide sufficient detail to permit organizations to rapidly recognize and respond to any terrorist event using WMD. Attachment 6 provides additional crisis action planning considerations that should be included in addressing terrorist use of WMD.

3.33.2.8. (Added) Force Protection Performance Measures (FPPMs). The Air Staff Security Forces/ Force Protection Division will develop, implement, track, and report the status of the Air Force's Force Protection Program (AF FPP). The purpose of the FPPMs is to mark milestones in the program, and as markers are met, FP measures will be discontinued and new ones established as needed. HQ USAF/ XOFP will identify measures to be reported by message to the MAJCOM semi-annually during October and April. HQ AFMC/SF will provide the FPPMs to the installation AT/FP Officer prior to the data call. The installation AT/FP Officer will collect and compile the information required by the FPPM and provide it to HQ AFMC/SF by the 15th day of the reporting month.

## Attachment 1
## GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

***References***

**DoDD 5200.39,** *Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection*

**AFJI 31-102**, *Physical Security*

**AFI 10-1011,** *Operations Security*

**Interim Department of Defense Antiterrorism/Force Protection Construction Standard**

**DTRA,** *Joint Staff Integrated Vulnerability Assessment Program Security Classification Guide, 1 Sept 97*

**Chem-bio Handbook,** *Janes*

**AFSFC/SFP CD ROM,** *Antiterrorism Reference Library*

**AFSFC/SFP CD ROM,** *Explosive Recognition 1 and 2*

***Terms***

**AT Awareness,—**Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorism. (Joint Pub 1-02)

**AT Resident Training,—**Formal classroom instruction in designated DoD courses that provide specialized instruction on specific combating terrorism topics; i.e., personal protection, terrorism analysis, regional interest, and AT/FP planning. (DoD Directive 2000.12)

**DoD Civilian Work Force,—**U.S. citizens or foreign nationals working for the Department of Defense, paid from appropriated or nonappropriated funds under permanent or temporary appointment. This includes employees filling full-time, part-time, intermittent, or on-call positions. Specifically excluded are all Government contractor employees. Contingency and emergency planning for contractor employees is covered by DoD Instructions 3020.37 and 1400.32)

**Defense Contractor,—**Any individual, firm, corporation, partnership, association, or other legal non-Federal entity that enters into a contract directly with the Department of Defense to furnish services, supplies, or both, including construction. Thus, Defense contractors may include U.S. nationals, local citizens, or third country nationals. Defense contractors do not include foreign governments or representatives of foreign governments that are engaged in selling to the Department of Defense or a DoD component or foreign corporations wholly-owned by foreign governments. (DoD Directive 2000.12)

**DoD-Designated High Physical Threat Countries,—**Countries determined to be of significant terrorist threat to DoD travelers, as designated by the ASD(SO/LIC), in coordination with the Assistant Secretary of Defense for International Security Affairs (ASD(ISA)) and the Assistant Secretary of Defense for International Security Policy (ASD(ISP)). DoD Directive 2000.12)

**Domestic Terrorism,—**Terrorism perpetrated by the citizens of one country against fellow countrymen. This includes acts against citizens of a second country when they are in the host country, and not the principal or intended target. (DoD Directive 2000.12)

**Family Member,—**"Dependent," as defined in 10 U.S.C., spouse; unmarried widow; unmarried widower; unmarried legitimate child, including adopted child or stepchild (over 18 but under 21),

incapable of self support or under 23 and enrolled in a full-time institution. (Section 1072(2) of title 10, United States Code)

**Military Service,—**A branch of the Armed Forces of the United States, established by act of Congress, in which persons are appointed, enlisted, or inducted for military service, and which operates and is administered within a Military or Executive Department. The Military Services are the United States Army, United States Navy, United States Air Force, United States Marine Corps, and the United States Coast Guard. (Joint Pub 1-02)

**No Double Standard Policy,—**Commanders may immediately disseminate to DoD personnel and facilities information on specific terrorist threats directed against DoD personnel and facilities. However, it is the policy of the United States Government that no double standard regarding availability of information will exist. Official Americans cannot benefit from receipt of information that might equally apply to the public, but is not available to the public. Responsibility for the release of threat information to the public in CONUS remains with the FBI and overseas with the Department of State. Threats directed against or affecting the American public, or against events/locales visited/utilized by the American public, will be coordinated with the FBI or DOS, as appropriate, prior to release. This policy applies only when the information available is sufficient for DoD activities to conclude that an act of terrorism will occur and to predict, with reasonable accuracy, the time, place, mode of the attack, and, if possible, the perpetrators. When such specificity exists, but it is impossible to determine that only Government targets might be affected, it is DoD policy that the reporting entity unilaterally disseminating the information will include both DoS and the AMEMBASSY or AMEMBASSIES concerned, on the message correspondence. The "No Double Standard" requirement for commanders at all levels is simple: keep either the American Embassy or the local office of the FBI informed of your threat levels and threat conditions. This can be accomplished through direct liaison if authorized or through the CINC via the chain of command. (DoD Directive 2000.12)

**Overseas Security Advisory Council (OSAC),—**OSAC was established by the Department of State in 1985 to foster the exchange of information between American companies with overseas operations and the U.S. Government. Government and business representatives have joined to use OSAC as a forum to produce a series of publications providing guidance, suggestions, and planning techniques on a variety of security-related issues, including terrorism.

## Attachment 6 (ADDED AFMC)
## WMD CRISIS ACTION PLANNING CONSIDERATIONS

**A6.1. Commander's estimate of the potential use of WMD:** This forms the basis for all facts and assumptions that drive the planning and preparation for any use of WMD by potential threat organizations. As such, the commander's estimate is the cornerstone of any successful program and must be reviewed frequently to incorporate any new or emerging threat.

**A6.2. Type/number of threats:** Accurate identification of the WMD threats posed by terrorist organizations provide a mechanism to determine the resources needed to counter the threat and respond effectively if they are used. Planners should also factor in the magnitude and diversity of the threats throughout an AOR.

**A6.3. Most likely/most vulnerable targets:** Most organizations can't provide total protection for all personnel and facilities in their AOR. However, identification of the most likely and vulnerable targets enables more detailed planning, which then drives responsible organizations to improve security measures. Further, responsible organizations can take measures to improve the security for these areas.

**A6.4. Target Value Analysis:** Certain areas pose different challenges from those above due to their specific value to terrorists. These targets may not be mission related or of high military value, but their value to terrorists may be very high. High use areas, such as shopping facilities or office complexes, have inherent problems with access control and usually have large concentrations of unprotected personnel present. Special analysis and planning should be done to help reduce the vulnerability of these type areas. This analysis must be conducted by fusing all available sources of information on the terrorist organizations.

**A6.5. Coordination with local authorities:** Coordination with local authorities is essential when planning for terrorist WMD use. It is likely that an attack on either the DoD facility or the local civilian populace will affect both communities. Dispersion of the agent affects by environmental factors (wind, water, or animals) can quickly spread to surrounding areas. Thorough coordination between DoD organizations and local officials provides a means to improve the response time and offers the opportunity to share critical resources needed to mitigate the effects of an attack.

**A6.6. Attack recognition and agent characterization:** Unless prior warning is obtained of an impending attack, most organizations will not have automatic detection devices and alarms in operation. Attack recognition may come only when symptoms first appear in exposed personnel. Agent identification will probably be done by first responders or medical personnel. Planning must address this potential vulnerability and incorporate procedures that minimize the delay from attack initiation until detection.

**A6.7. Warning systems:** Because WMD attacks can cover large areas, timely warning can reduce the number of personnel who would otherwise be exposed to agent effects. A combination of outdoor warning sirens, telephonic notification, and broadcast announcements provide redundant warning systems that will reach a large portion of the population. Special consideration should be given to unique populations, such as the visually or hearing impaired, to ensure effective warning systems are in place to provide for their safety.

**A6.8. Response levels:** Different agents require different responses. Plans should include details on the appropriate response for the agents identified in the commander's assessment and the equipment needed to implement that level of response.

**A6.9. Hazardous Material Response Teams:** Federal, state and local regulations have specific requirements for personnel responding to hazardous material and substances. Commanders must be aware of

these requirements and emergency responders must have the equipment and training necessary to protect themselves, treat casualties and decontaminate the site. Planning should include adequate time and resources to ensure response teams have the appropriate equipment and level of training.

**A6.10. Reporting procedures:** Because of the sensitivity of terrorist use of WMD, many agencies require formatted reports on the nature of the event. Plans should include preformatted templates for reporting requirements; message addresses and phone numbers for the agencies and commands that must be notified. Communications can rapidly overload available communications means during a crisis. Brevity codes, established crisis action communication procedures and predetermined local reporting requirements will all assist in the management of a crisis by providing timely and accurate information to the emergency operations center.

**A6.11. Crisis action team responsibilities:** Emergency operations centers normally have only a small staff on duty and will require immediate augmentation when an attack occurs. Staff elements should be fully trained and prepared to implement the appropriate plan to reduce the effects of the WMD attack. It may be necessary to operate in protective equipment during the initial states of the crisis. Training on the use of protective equipment and their specific duties as part of the emergency operations center staff should be regularly exercised to maintain proficiency in crisis action responsibilities.

**A6.12. First responder responsibilities:** First responders will be called on to perform many critical functions during a WMD attack. Law enforcement, fire, medical, explosive ordnance disposal and facility engineer teams will usually be some of the first organizations to react to an event. Careful planning and training is needed to address the special needs of these groups. The actions they take during the initial stages of an event will have a very important impact on the consequence management steps that follow.

**A6.13. Medical support, treatment and transportation requirements:** Prior coordination with state and local medical facilities is necessary to ensure medical plans include procedures to treat and care for contaminated or infected personnel. Personnel who treat contaminated casualties or handle contaminated remains require special training. Medical facilities should have areas designated to treat and segregate contaminated patients. Preventive medicine specialists and pathologists need to have a database of naturally occurring diseases and procedures to quickly assess and identify suspicious illnesses and diseases. Antidotes and treatments for potential agents from commercial or industrial sources should be considered in the casualty management plan. Contaminated patient transport and contamination control measures should be incorporated into litter and ambulance operations.

**A6.14. Temporary Shelters, Evacuation routes and care centers:** There will always be a requirement to clear an area and provide orderly evacuation to safe areas when WMD is used. Temporary shelters, evacuation routes, and care centers should be identified during the planning process. Commanders should identify facilities for potential use in defense against chemical, radiological, and biological agents. Existing facilities may be suitable for adaptation as temporary shelters/toxic-free areas, since sufficient collective protection resources may be inadequate. Law enforcement and security personnel need to determine traffic control points to facilitate evacuation and prevent personnel from entering potentially contaminated areas. Copies of the routes and locations of care centers should be available to installation workers and residents.

**A6.15. Public affairs:** The demand for information from the public and the media will be intense at the onset of an event. Public affairs planning should include background information on the potential agents and materials that pose a threat. Basic information on the properties, effects, treatment, duration, and decontamination of likely threat agents should be included in the public affairs reference materials

brought to the emergency operations center and joint information center. Rapid and accurate information on the hazard during the early stages of an event will assist in protecting civilians from the hazard and foster confidence in DoD's ability to safely manage the crisis.

**A6.16. Crime scene procedures for agent material:** Terrorist use of any WMD material is a criminal act. Local plans should include procedures to control a crime scene in a contaminated environment and provide for the recovery of evidence that may be hazardous. For domestic events, the FBI will be responsible for investigating the criminal incident. Law enforcement and security plans should provide procedures to facilitate the transition of responsibility when FBI arrives on site.

**A6.17. Follow-on assistance:** Any WMD event will generate the requirements for some form of external support or assistance. Plans should determine the type, amount and time frame for follow-on assistance. The logistics of managing a large contingent of external support organizations has the potential of overwhelming the ability of the local commander to control its effective employment.

**A6.18. Hazard prediction:** When an event occurs, there is an immediate need to predict the size of the potential hazard zone. Reports from first responders will contain the location of the incident site; but the initial estimate of the hazard area should be made by emergency operations center personnel. Procedures should be incorporated into emergency operations centers that allow for a quick initial hazard prediction and methods for its rapid dissemination. Detailed predictions can be made when more information is provided on the agent type and dissemination means.

**A6.19. Meteorological support:** As indicated above, hazard prediction must be done quickly. Current and reliable weather data is critical to providing accurate hazard predictions. Updated weather data should be routinely provided to emergency operations centers so that it is available at the onset of an event. Organizations providing data should be part of the planning process so they can develop weather products that support hazard prediction models or programs.

**A6.20. Contamination control:** Containing and limiting the spread of contamination is essential in reducing the effects of a WMD attack. Procedures for personnel responding to the attack site should include methods that minimize their direct contact with contaminated material. Work crews should use sumps to collect runoff from decontamination operations. Access into the site should be through designated points and along designated routes.

**A6.21. Decontamination and hot line operations:** Decontamination procedures should be developed using the resources locally available. Decontaminating exposed personnel, first responders, and site work teams requires the rapid establishment of a decontamination site. Plans should consider the requirement to maintain decontamination operations for extended periods and the potentially large personnel and logistics need generated to support this type of operation.

**A6.22. Sampling and analysis:** Sampling will be required at the attack site and in the predicted hazard areas to establish the presence or absence of contamination. Plans should include procedures to determine sampling requirements and protocols for the collection of agent material. Analysis may be done locally at the onset of an attack, buy may be shipped off-site for confirmation or for detailed analysis if local facilities cannot identify the material.

**A6.23. Monitoring operations:** Monitoring plans should include procedures to employ detection equipment to known or suspected hazard locations. Detection equipment intended for military tactical level employment may not detect agent concentrations that are considered hazardous by the EPA, Occupational Safety and Health Administration and the Nuclear Regulatory Agency. Environmental and safety plan-

ners must be aware of the hazardous material exposure limits of civilian populations and understand the limitations of using military equipment to determine when areas are considered free of contamination.

**A6.24. Reentry and remediation operations:** Preliminary planning should address the considerations for these operations. Reentry includes actions required to permit personnel to safely enter an area following an attack. Remediation includes actions to remove all contamination from the site and restore the environment to its original condition. Both of these processes can potentially take several days to weeks to complete. External support will probably be needed to ensure these tasks are properly accomplished.

**A6.25. Training** Training programs should provide a comprehensive approach to meeting the needs identified in mitigation efforts. Actions required to reduce the vulnerability to attack and to respond as the result of a terrorist WMD incident involve many different tasks and levels of training. At a minimum, training programs should include individual, first responder, functional response team, and emergency operations center training.

HUBERT G. MITCHELL, Colonel, USAF
Director, Security Forces